http://ourworld.compuserve.com/homepages/ckune r/multimd 3. htm. 7. Доступ до інформації та електронне урядування / Автори-упорядники М. С. Демкова, М. В. Фігель. — К.: Факт, 2004. — 336 с.

УДК 681.3:34

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХОДІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Євген Скулиш, Дарія Прокоф'єва
Головне управління по боротьбі з корупцією та організованою злочинністю СБ України

Анотація: **Подається огляд законодавчого забезпечення інформаційної безпеки при здійсненні оперативно-розшукової діяльності в Україні та інших країнах Європи.**
Summary: **This article represents the review of the ways of information security's supplying by the law during detective activity in Ukraine and other European countries.**
Ключові слова: **Законодавство, інформаційна безпека, оперативно-розшукова діяльність.**

Як складова метасистеми національної безпеки країни інформаційна безпека людини перебуває в тісному взаємозв'язку з рештою її складових – безпекою держави та суспільства. Вона забезпечується при дотриманні спільних для всієї системи принципів: законності, балансу життєво важливих інтересів особи, суспільства та держави, їх взаємної відповідальності щодо забезпечення безпеки та інтеграції з міжнародними системами безпеки, тощо. При цьому інформаційна безпека людини потрапляє до сфери оперативно-розшукової діяльності, яка різнобічно впливає на неї [1 – 2].

З одного боку, оперативно-розшукова діяльність покликана захищати життєво важливі інтереси людини в інформаційній сфері від внутрішніх та зовнішніх загроз. Це здійснюється шляхом виявлення, попередження, припинення та розкриття злочинів, що посягають на законні інформаційні інтереси особи, перш за все – на конституційні права та свободи людини і громадянина в цій сфері, а також шляхом здобуття інформації про події та дії, що створюють загрозу державній, військовій, економічній, екологічній або іншій складовій національної безпеки, оскільки це також безпосередньо пов'язано з забезпеченням інформаційної безпеки людини [3 – 4].

З іншого боку, власне оперативно-розшукова діяльність може створювати загрозу інформаційній безпеці людини у випадках:

- здійснення оперативно-розшукової діяльності без достатніх підстав або з порушеннями встановленого порядку проведення оперативно-розшукових заходів, особливо таких, що обмежують конституційні права та свободи людини і громадянина;
- використання одержаної в результаті проведення оперативно-розшукових заходів інформації для вирішення завдань, що виходять за межі компетенції органів, які здійснюють оперативно-розшукову діяльність (передусім мова йде про незаконне поширення інформації про особу);
- необґрунтованої відмови в наданні особі відомостей щодо отриманої про неї інформації або незаконне обмеження її в ознайомленні з такими відомостями;
- порушення вимог конспірації та режиму таємності інформації щодо осіб, які конфіденційно співробітничають або співробітничали з органами, що здійснюють оперативно-розшукову діяльність [4].

Вище йшлося про зловживання владою і повноваженнями як причину порушення балансу інтересів особи, суспільства та держави в інформаційній сфері. Однак в окремих випадках власне сам характер протиправних діянь, а також специфіка їх суб'єктів зумовлює конфлікт відповідних інтересів в інформаційній сфері. В свою чергу, це вимагає від правоохоронних органів застосування оперативно-розшукових заходів, які обмежують конституційні права і свободи громадян з метою забезпечення правопорядку та безпеки держави і суспільства. Передусім мова йде про зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, кореспонденцією тощо, застосування інших технічних засобів одержання інформації [4].

Відповідно до стандартів Європейського суду з прав людини для того, щоб перехоплення телефонного повідомлення або інший контроль кореспонденції не вважалися порушенням ст. 8 Європейської Конвенції про захист прав людини та основних свобод [5 – 6], воно має здійснюватися на підставі закону та як необхідне в демократичному суспільстві. Здійснення перехоплення повідомлення на підставі закону означає, що будь-яке спостереження за кореспонденцією має здійснюватися відповідно до закону, що відповідає вимогам доступності, передбачуваності та якості. За змістом принципу доступності «громадянин повинен мати можливість пересвідчитись, що прослуховування відповідає законодавчим

нормам, що використані в даному конкретному випадку». Передбачуваність означає, що громадянин має бути здатний (в разі необхідності – за допомогою адвоката) передбачити наслідки будь-якої можливої дії. Закон також повинен передбачати адекватні та ефективні перешкоди можливим зловживанням, зокрема: визначати перелік злочинів, вчинення яких може призвести до прослуховування; обмежуватись випадками, коли фактичні підстави підозрювати особу у вчиненні тяжкого злочину вже виявлені іншими засобами; санкціонувати прослуховування лише на підставі мотивованого письмового звернення певної високопоставленої посадової особи; дозволяти проведення прослуховування тільки після отримання санкції орагана або посадової особи, що не належить до виконавчої влади, бажано – судді; встановлювати обмеження на тривалість прослуховування, тобто, має бути вказаний період, протягом якого санкція на прослуховування є чинною; передбачати запобіжні заходи проти обміну матеріалами, здобутими за результатами прослуховування, між різними державними органами; визначати обставини, за яких відповідні матеріали можливо або необхідно знищувати; встановлювати, що робити з копіями або відтвореними матеріалами, якщо обвинуваченого буде виправдано судом.

Як необхідне в демократичному суспільстві прослуховування розглядається тоді, коли здійснюється лише в тій мірі, в якій воно необхідне для безпеки демократичних інститутів, а також за виключних умов – в інтересах національної безпеки та/або попередження заворушень та злочинів.

Слід зазначити, що під визначення кореспонднції за змістом Європейської Конвенції про захист прав людини та основних свобод підпадають не лише розмови і повідомлення, але й їхній хронометраж [6].

Наведені стандарти зумовили вдосконалення законодавства країн – членів Ради Європи, яке регламентувало процедури зняття інформації з каналів зв‘язку.

Зокрема, після того, як Європейський Суд з прав людини виявив, що внутрішнє законодавство Франції порушує Конвенцію, в 1991 році було прийнято Закон про недоторканість кореспонденції, що передається засобами телекомунікацій, специфічним положенням якого є заборона на прослуховування домашніх та службових телефонів адвокатів, якщо про це не буде повідомлений президент Асоціації юристів Франції [6].

Конституція Швеції забороняє перехоплення кореспонденції або нагляд за нею крім випадків, коли це передбачено законом в інтересах демократичного суспільства. Такими законами є Судовий процесуальний кодекс та Закон 1952:98, який містить окремі правила щодо примусових заходів і використовується Поліцією Безпеки Швеції. Дозвіл на прослуховування або нагляд за кореспонденцією надається судом за поданням прокурора виключно з метою попередити злочин або підготовку до його вчинення і лише у випадках, коли іншими засобами запобігти злочинові неможливо. Законодавство Швеції покладає на компанії зв‘язку обов‘язок щодо конструювання та експлуатації ліній зв‘язку таким чином, щоб можливо було забезпечити виконання відповідних примусових заходів за рішенням суду. Після завершення вказаних заходів піднаглядна особа не має права дізнатися про те, що вони щодо неї здійснювалися [6].

Конституція Угорщини не містить положень щодо недоторканості особистої кореспонденції. Водночас, Акт N CXXV 1995 року про національні служби безпеки регламентує процедуру прослуховування телефонних розмов, яке дозволяється у випадку виникнення загрози національній безпеці з дозволу Міністра юстиції або суду за поданням генерального директора відповідної правоохоронної служби. Під загрозою національній безпеці розуміють загрозу незалежності або територіальній цілісності країни, таємні спроби підірвати економічну, політичну або військову міць країни, незаконно змінити або порушити конституційний лад, зрада, тероризм, контрабанда зброї та наркотиків, незаконне розповсюдження виробів і технологій, що перебувають під міжнародним контролем. Однією з особливостей оформлення подання для отримання дозволу на зняття інформації з каналів зв‘язку є необхідність зазначення в тексті подання спеціальних засобів, що будуть використовуватись при проведенні відповідного примусового заходу [6].

Відповідно до прийнятого в 1990 році Сеймом Польщі Закону про Службу захисту держави (в редакції 1995 року), Міністр внутрішніх справ може подати Генеральному прокуророві запит для надання письмової згоди на прослуховування телефонних розмов з метою встановлення фактів та протидії загрозам національній безпеці, обороні, суверенітету та цілісності держави, шпигунству, тероризму та іншим тяжким злочинам проти держави, а також розкриттю державних секретів. Прослуховування дозволяється також для попередження та розкриття злочинів проти основних політичних та економічних інтересів Республіки Польща, підкупу офіційних осіб, злочинів, що караються за міжнародними договорами або угодами тощо. В екстрених випадках лінії зв‘язку можуть прослуховуватись за наказом Міністра внутрішніх справ до отримання дозволу Генерального прокурора протягом 24 годин. Крім того, Кримінально-процесуальний кодекс передбачає обов‘язок для закладів пошти, відділень зв‘язку на вимогу суду та прокурора видавати будь-яку кореспонденцію, що має значення для розслідування кримінальної справи [6].

В Румунії норми, що визначають процедуру законності прослуховування, містяться в Кримінально-процесуальному кодексі та в Законі про національну безпеку від 1991 року. Підставою для встановлення прослуховування прокурором на запит компетентних органів безпеки є вчинення або підготовка до вчинення державної зради, збройного повстання, політичного вбивства, тероризму, викрадення зброї, боєприпасів, вибухових та радіоактивних речовин, токсичних або бактеріологічних матеріалів та торгівля ними, а також знищення, пошкодження або приведення до непридатного стану структур, необхідних для нормального розвитку громадського життя або національної безпеки, розголошення державних секретів або їх недбале зберігання, участь в тоталітарних або екстремістських діях та виступах тощо. Зауважимо, що запит бажано, але не обов'язково має містити відомості про особу, розмови якої планується прослуховувати. В разі термінової необхідності прослуховування може здійснюватись і без дозволу прокурора, який втім слід отримати протягом наступних 48 годин [6].

Німеччина стала єдиною країною, чинні норми якої щодо перехоплення кореспонденції схвалив Європейський суд з прав людини. Підстави та процедура зняття інформації з каналів зв'язку визначаються Законом про обмеження конфіденційності поштових та електронних відправлень, який на виконання конституційних норм було прийнято ще в 1968 році. Так, прослуховування та перехоплення кореспонденції допускається у випадку збройного нападу на Німеччину, а також для викриття та припинення злочинів проти миру, державної зради, підриву демократичного ладу та законності, шпигунства та загроз національній безпеці, злочинів проти національної обороноздатності, військ НАТО, забороненої діяльності, вбивств, геноциду, викрадення людей з метою викупу, захоплення заручників, знищення майна шляхом підпалів, вибухів в транспортних засобах та отруєння. Ордер на перехоплення кореспонденції видається лише щодо осіб, які, згідно з встановленими фактами, «отримують або передають інформацію з метою вийти з-під підозри», причому отримані в результаті перехоплення кореспонденції відомості можуть вважатися допустимими джерелами доказів за умови, що інші способи встановлення відповідних фактів ускладнені або унеможливлені. В будь-якому разі такі відомості не можуть використовуватись «на шкоду особам, що перебували під спостереженням» [6].

Водночас слід зазначити, що активізація терористичних проявів для багатьох європейських країн зумовила зміщення акцентів національної (в т. ч. – інформаційної) безпеки із безумовного та першочергового дотримання privacy на забезпечення безпеки суспільства та держави. Зокрема, в 2003 році Конституційний суд Німеччини уповноважив поліцію відстежувати телефонні дзвінки журналістів «у серйозних випадках» [7]. З 2004 року впровадження відповідних антитерористичних заходів розпочато також у Великобританії, Франції тощо [8 – 9].

Відповідно до статті 31 Конституції України кожному гарантується таємниця телефонних розмов. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо [10]. Це положення Основного Закону України деталізується у нормах Кримінально-процесуального кодексу України [11], законах України "Про оперативно-розшукову діяльність" [4], "Про боротьбу з тероризмом" [12], "Про державний захист працівників суду і правоохоронних органів" [13], "Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» [14]. Зокрема, відповідно до вимог частини другої статті 8 Закону "Про оперативно-розшукову діяльність" зняття інформації з каналів зв'язку, контроль за телефонними розмовами проводяться за рішенням суду, прийнятим за поданням керівника відповідного оперативного підрозділу або його заступника. Про отримання такого дозволу суду або про його відмову в ньому визначені особи повідомляють прокуратуру протягом доби. Застосування цих заходів проводиться виключно з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо. За результатами здійснення зазначених оперативно-розшукових заходів складається протокол з відповідними додатками, який підлягає використанню як джерело доказів у кримінальному судочинстві [4, 6].

Вказаними законодавчими актами визначаються підстави та порядок проведення зазначених оперативно-розшукових заходів, контроль, прокурорський нагляд та гарантії законності під час їх здійснення. Загалом відповідаючи вимогам Європейського суду з прав людини, вітчизняне законодавство не містить прозорої регламентації процедури отримання дозволу на зняття інформації з каналів зв'язку. Не достатньо також окреслено порядок використання результатів проведених відповідних оперативно-розшукових заходів в кримінальному судочинстві. Ці недоліки мають бути виправлені в ході подальшої інтеграції України до Європейського співтовариства виходячи з потреб дотримання балансу інтересів особи, суспільства та держави в інформаційній сфері та забезпечення інформаційної безпеки зазначених суб'єктів.

В цілому ж система забезпечення інформаційної безпеки України має будуватися на основі дотримання

конституційних норм щодо недоторканості приватного життя та конфіденційності кореспонденції, оскільки права і свободи людини та громадянина мають найвищій пріоритет, а власне система національної безпеки є найбільш дієвим механізмом забезпечення безпеки людини.

Література: ***1.*** *Ліпкан В. А. Національна безпека України у світлі теорії самоорганізації // Держава і право. - 2002. - № 16. - С. 142 – 148.* ***2.*** *Ліпкан В. (n. d. / 2003). Націобезпекознавча парадигма // Право України. - 2003 рік, №2 [WWW документ]. URL http:// www.refua.narod.ru (12 листопада 2004).* ***3.*** *Рябчук В. Н. (18. 10. 2000). Информационная безопасность человека и оперативно-розыскная деятельность // Материалы научной конференции "Концептуальные проблемы информационной безопасности в союзе России и Беларуси". – СПб., 2000 [WWW документ]. URL http:// jurfak.spb.ru/conference/2001.htm (11 вересня 2003).* ***4.*** *Верховна Рада України (18 .02 .1992). Закон України "Про оперативно-розшукову діяльність" від 18 лютого 1992 р. [WWW документ]. URL http:// www.rada.kiev.ua (29 вересня 2006).* ***5.*** *Council of Europe (n. d. / 2002). Европейская конвенция о защите прав человека: право и практика [WWW документ]. URL http:// www.echr.ru (20 вересня 2006 р.)* ***6.*** *Харьковская правозащитная группа (n. d. / 1999). Прослушивание телефонов в международном праве и законодательстве 11 европейских стран. [WWW документ]. URL http:// www.mtc.ana/news/news, 47.htm (29 вересня 2006).* ***7.*** *Конституционный суд Германии разрешил полиции прослушивать телефоны журналистов. – 2003 03. 24 [WWW документ]. URL http:// media.topping.com.ua/news/sosiety/2003/03/24/ 149229. htm (20 вересня 2006 р.)* ***8.*** *Французская полиция получила дополнительные полномочия. – 2004. 10. 01 [WWW документ]. URL http: // www.iter-tass.com/russ/newsdir.html (20 вересня 2006 р.)* ***9.*** *В условиях напряженности и настороженности, охвативших Великобританию после прошедших терактов, Премьер-министр Тони Блэр выступил с инициативой принятия действенных законодательных мер, способных поставить заслон на пути террористов/ - 2005. 07. 27 [WWW документ]. URL http:// www.pravo.by/news.asp* ***10.*** *Конституція України // Закони України. - К., 1997. – Т.10. – 335 с.* ***11.*** *Верховна Рада УРСР (28. 12. 1960). Кримінально-процесуальний кодекс України від 28 грудня 1960 р. (28. 12. 1960). [WWW документ]. URL http:// www.rada.kiev.ua (29 вересня 2005).* ***12.*** *Верховна Рада України (20. 03. 2003). Закон України "Про боротьбу з тероризмом" від 20 березня 2003 р. (20. 03. 2003). WWW документ]. URL http:// www.rada.kiev.ua (29 вересня 2005).* ***13.*** *Верховна Рада України (23. 12. 1993). Закон України «Про державний захист працівників суду і правоохоронних органів"від 23 грудня 1993 р. (23. 12. 1993). [WWW документ]. URL http://www.rada.kiev.ua (29 вересня 2005).* ***14.*** *Верховна Рада України (23. 12. 1993). Закон України "Про забезпечення безпеки осіб, які беруть участь в кримінальному судочинстві" від 23 грудня 1993 р. (23. 12. 1993). [WWW документ]. URL http:// www.rada.kiev.ua (29 вересня 2005).*

УДК 681.391

АНАЛИЗ РЕЗУЛЬТАТОВ АРТИКУЛЯЦИОННЫХ И СЕГМЕНТАЛЬНЫХ ИСПЫТАНИЙ СИГНАЛОВ МАСКИРОВАНИЯ РЕЧИ

Михаил Прокофьев, Владимир Журавлёв*

*Национальный технический университет Украины «КПИ», *Запорожский национальный технический университет*

Анотація: **Розглянуто методику та результати випробувань цифрової кореляційної обробки контрольного фрагменту мови, що дозволяє на основі розрахунку коефіцієнта кореляції обґрунтувати аналітичну оцінку параметра якості передачі сигналу мови каналами зв'язку та проводити аналіз ефективності адитивного маскування мовних сигналів.**

Summary: **The method of check utterance digital correlation processing, which allows to substantiate the communication path quality criteria analytic estimation on the base of correlation coefficient calculation and to analyze the speech signal additive masking effectiveness is under review.**

Ключевые слова: **Речевой сигнал, речеподобный шум, аддитивное маскирование, корреляционная обработка, параметр качества.**

I Введение

Акустическая и виброакустическая защита выделенных помещений от несанкционированного доступа представляет собой сегодня одно из наиболее динамично развивающихся направлений комплексной